

UNITED STATES DISTRICT COURT
for the
Southern District of California

CLERK US DISTRICT COURT
SOUTHERN DISTRICT OF CALIFORNIA
BY DEPUTY

JUL 24 2019

In the Matter of the Search of
(Briefly describe the property to be searched
or identify the person by name and address)
An Apple iPhone XS, IMEI No. 862998037340728
)

Case No.

19MJ3086

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):

See Attachment A, which is incorporated by reference.

located in the Southern District of California, there is now concealed (identify the person or describe the property to be seized):

See Attachment B, which is incorporated by reference.

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

evidence of a crime;
 contraband, fruits of crime, or other items illegally possessed;
 property designed for use, intended for use, or used in committing a crime;
 a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

<i>Code Section</i>	<i>Offense Description</i>
21 U.S.C. §§ 952, 960 and 963	Importation of controlled substances and conspiracy to do the same

The application is based on these facts:

See Affidavit of HSI Special Agent Allie Peters, which is hereby incorporated by reference and made part hereof.

Continued on the attached sheet.
 Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.



Applicant's signature

Special Agent Allie Peters, HSI

Printed name and title



Judge's signature

Sworn to before me and signed in my presence.

Date: 7-24-2019 @ 9:00 am

City and state: San Diego, CA

Hon. Peter C. Lewis, U.S. Magistrate Judge

Printed name and title

AFFIDAVIT

I, Special Agent Allie Peters, being duly sworn, hereby state as follows:

INTRODUCTION

1. I submit this affidavit in support of an application for a warrant to search an Apple iPhone XS, IMEI No. 862998037340728 (the “Target Device”), and seize evidence of crimes, specifically violations of Title 21, United States Code, Section(s) 952, 960, and 963. The requested warrant relates to the investigation and prosecution of Priscilla Gonzalez (“Defendant”) for importing approximately 36.90 kilograms (81.35 pounds) of cocaine from Mexico into the United States. *See U.S. v. Gonzalez*, Case No. 19-mj-2547 (S.D. Cal.) at ECF No. 1. (Complaint). The Target Device is currently in the possession of Homeland Security Investigations, 2255 Niels Bohr Ct., San Diego, CA, 92154.

2. The information contained in this affidavit is based upon my experience, training, investigation, and consultation with other members of law enforcement. Because this affidavit is made for the limited purpose of obtaining a search warrant for the Target Device, it does not contain all the information known by me or other agents regarding this investigation.

BACKGROUND

3. I have been employed as a Special Agent with Homeland Security Investigations (HSI) since August 2018. Prior to becoming a Special Agent, I served as a Customs and Border Protection (CBP) Officer from 2015-2018.

4. I have completed and graduated from the twelve-week Criminal Investigator Training Program and the fifteen-week Homeland Security Investigations Special Agent Training Program at the Federal Law Enforcement Training Center in Glynco, Georgia. I have also completed and graduated from the four-month Officer Basic Training Academy for CBP Officers.

5. Since April 2019, I have been assigned to a Narcotics Response Group in San Ysidro, CA. My duties include investigating the illicit trafficking of controlled substances into and within the United States. During my assignment to the Narcotics Response Group,

1 I have participated in the investigation of various drug trafficking organizations involved
2 in the importation and distribution of controlled substances into and through the Southern
3 District of California.

4 6. Through my training, experience, and conversations with other members of
5 law enforcement, I have gained a working knowledge and insight into the operational
6 habits of narcotics traffickers, in particular those who attempt to import narcotics into the
7 United States from Mexico at Ports of Entry. I am aware that it is common practice for
8 narcotics smugglers to work in concert with other individuals and to do so by utilizing
9 cellular telephones. The use of cellular telephones permits narcotics traffickers to remotely
10 do things on demand such as actively monitor the progress of their illegal cargo while it is
11 in transit, arrange for the delivery of contraband at predetermined locations, direct drug
12 couriers to synchronize drop off and pick up times, notify or warn accomplices about law
13 enforcement activity, and communicate with co-conspirators who are transporting their
14 narcotics and/or proceeds from narcotics sales.

15 7. Based upon my training, experience, and consultations with law enforcement
16 officers experienced in narcotics trafficking investigations, and all the facts and opinions
17 set forth in this affidavit, I know that cellular telephones can and often do contain electronic
18 evidence, including, for example, phone logs and contacts, voice and text communications,
19 and data, such as emails, text messages, chats and chat logs from various third-party
20 applications, photographs, audio files, videos, and location data. This information can be
21 stored within disks, memory cards, deleted data, remnant data, slack space, and temporary
22 or permanent files contained on or in the cellular/mobile telephone. Specifically, searches
23 of cellular telephones may yield evidence:

24 a. tending to indicate efforts to import cocaine, or some other federally
25 controlled substance, from Mexico into the United States;

26 b. tending to identify accounts, facilities, storage devices, and/or services—
27 such as email addresses, IP addresses, and phone numbers—used to
28 facilitate the importation of cocaine, or some other federally controlled
substance, from Mexico into the United States;

- 1 c. tending to identify co-conspirators, criminal associates, or others involved
- 2 in importation of cocaine, or some other federally controlled substance,
- 3 from Mexico into the United States;
- 4 d. tending to identify travel to or presence at locations involved in the
- 5 importation of cocaine, or some other federally controlled substance, from
- 6 Mexico into the United States, such as stash houses, load houses, or
- 7 delivery points;
- 8 e. tending to identify the user of, or persons with control over or access to,
- 9 the Target Device; and/or
- 10 f. tending to place in context, identify the creator or recipient of, or establish
- 11 the time of creation or receipt of communications, records, or data involved
- 12 in the activities described above.

FACTS SUPPORTING PROBABLE CAUSE

13 8. Based on the initial reports from Customs and Border Protection (CBP)
14 Officers, on June 18, 2019, at approximately 10:25 a.m., defendant Priscilla Gonzalez
15 ("Defendant") applied for permission to enter the United States at the San Ysidro,
16 California Port of Entry. Defendant was driving a 2016 Honda Civic, and she was the only
17 person in her car. While in pre-primary, a narcotics detection canine alerted to the rear of
18 Defendant's vehicle, and she was referred for secondary inspection. During secondary
19 inspection, CBP Officers discovered 32 packages (18 in the doors and 14 in the back seats)
20 concealed within Defendant's vehicle. The packages weighed approximately 36.90 kg
21 (81.35 lbs.), and field-tested positive as cocaine. Defendant was subsequently arrested and
22 the Target Device was seized from Defendant's person.

23 9. During Defendant's post-arrest interview, I read Defendant her *Miranda*
24 rights and she agreed to waive them and speak to agents without an attorney. Defendant
25 told me that she responded to a Facebook advertisement and that her job was to cross the
26 vehicle into the United States. Defendant stated that she was instructed to deliver her
27 vehicle to a mechanic's shop in Mexico prior to crossing into the United States and to leave
28 her vehicle key hidden on a tire. Defendant stated that she was to be paid \$3,000 for her

1 efforts. Defendant further indicated that she expected to be contacted on her phone,
2 specifically through Facebook messenger, to be given a drop-off location for the car in the
3 United States.

4 10. Given Defendant's statements and my own experience and training, there is
5 probable cause to believe that Defendant was using the Target Device to communicate with
6 others to further an attempt to import illicit narcotics into the United States. In addition, in
7 my training and experience, narcotics traffickers may be involved in the planning and
8 coordination of a drug smuggling event in the days and weeks prior to an event. Further,
9 co-conspirators are often unaware of a defendant's arrest and will continue to attempt to
10 communicate with the defendant after the arrest to determine the whereabouts of the
11 narcotics. Based on my training and experience, it is also not unusual for individuals, such
12 as Defendant, to attempt to minimize the amount of time they were involved in their
13 smuggling activities, and for the individuals to be involved for weeks and months longer
14 than they claim. Accordingly, I request permission to search the Target Device for data
15 beginning on March 18, 2019, up to and including June 18, 2019.

METHODOLOGY

17 11. It is not possible to determine, merely by knowing the cellular telephone's
18 make, model and serial number, the nature and types of services to which the device is
19 subscribed and the nature of the data stored on the device. Cellular devices today can be
20 simple cellular telephones and text message devices, can include cameras, can serve as
21 personal digital assistants and have functions such as calendars and full address books and
22 can be mini-computers allowing for electronic mail services, web services and rudimentary
23 word processing. An increasing number of cellular service providers now allow for their
24 subscribers to access their device over the internet and remotely destroy all of the data
25 contained on the device. For that reason, the device may only be powered in a secure
26 environment or, if possible, started in "flight mode" which disables access to the network.
27 Unlike typical computers, many cellular telephones do not have hard drives or hard drive
28 equivalents and store information in volatile memory within the device or in memory cards

1 inserted into the device. Current technology provides some solutions for acquiring some of
2 the data stored in some cellular/mobile telephone models using forensic hardware and
3 software. Even if some of the stored information on the device may be acquired
4 forensically, not all of the data subject to seizure may be so acquired. For devices that are
5 not subject to forensic data acquisition or that have potentially relevant data stored that is
6 not subject to such acquisition, the examiner must inspect the device manually and record
7 the process and the results using digital photography. This process is time and labor
8 intensive and may take weeks or longer.

9 12. Following the issuance of this warrant, I will collect the subject cellular
10 telephone and subject it to analysis. All forensic analysis of the data contained within the
11 telephone and its memory cards will employ search protocols directed exclusively to the
12 identification and extraction of data within the scope of this warrant.

13 13. Based on the foregoing, identifying and extracting data subject to seizure
14 pursuant to this warrant may require a range of data analysis techniques, including manual
15 review, and, consequently, may take weeks or months. The personnel conducting the
16 identification and extraction of data will complete the analysis within ninety (90) days,
17 absent further application to this court.

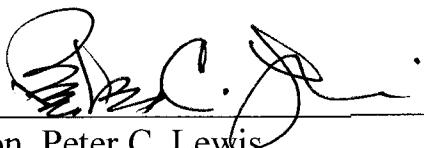
CONCLUSION

19 14. Based on the facts and information set forth above, there is probable cause to
20 believe that a search of the Target Device will yield evidence of Defendant's violations of
21 Title 21, United States Code, Section(s) 952, 960, and 963. Accordingly, I request that the
22 Court issue a warrant authorizing law enforcement to search the items described in
23 Attachment A and seize the items listed in Attachment B using the above-described
24 methodology.

1 I swear the foregoing is true and correct to the best of my knowledge and belief.
2
3

4 
5 Special Agent Allie Peters
6 Homeland Security Investigations
7

8 Subscribed and sworn to before me this 24 day of July, 2019.
9

10 
11 Hon. Peter C. Lewis
12 United States Magistrate Judge
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

ATTACHMENT A

PROPERTY TO BE SEARCHED

The following property is to be searched:

Apple iPhone XS
IMEI No. 862998037340728
(the "Target Device")

The Target Device is currently in the possession of Homeland Security Investigations, 2255 Niels Bohr Ct., San Diego, CA, 92154.

ATTACHMENT B

ITEMS TO BE SEIZED

Authorization to search the cellular telephone described in Attachment A includes the search of disks, memory cards, deleted data, remnant data, slack space, and temporary or permanent files contained on or in the cellular telephone for evidence described below. The seizure and search of the cellular telephone shall follow the search methodology described in the affidavit submitted in support of the warrant.

The evidence to be seized from the cellular telephone will be electronic records, communications, and data such as emails, text messages, chats and chat logs from various third-party applications, photographs, audio files, videos, and location data, for the period of March 18, 2019, up to and including June 18, 2019:

- a. tending to indicate efforts to import cocaine, or some other federally controlled substance, from Mexico into the United States;
- b. tending to identify accounts, facilities, storage devices, and/or services—such as email addresses, IP addresses, and phone numbers—used to facilitate the importation of cocaine, or some other federally controlled substance, from Mexico into the United States;
- c. tending to identify co-conspirators, criminal associates, or others involved in importation of cocaine, or some other federally controlled substance, from Mexico into the United States;
- d. tending to identify travel to or presence at locations involved in the importation of cocaine, or some other federally controlled substance, from Mexico into the United States, such as stash houses, load houses, or delivery points;
- e. tending to identify the user of, or persons with control over or access to, the Target Device; and/or
- f. tending to place in context, identify the creator or recipient of, or establish the time of creation or receipt of communications, records, or data involved in the activities described above;

which are evidence of violations of Title 21, United States Code, Sections 952, 960, and 963.